EXHIBIT J

From: Breslin, Mike <mbreslin@kilpatricktownsend.com>
Sent: Thursday, January 7, 2021 2:14 PM
To: Gallo, Joseph; LaVigne, Christopher
Cc: Wiley, Adam
Subject: ESI term comments
Attachments: Williams v. AT&T - Comments to Pl_s Proposed ESI Search Terms.DOCX

CAUTION: This email originated from an external source.

Joe / Chris –

Let me know if my comments appear in this one. Apologies they weren't in the previous version I sent.

-Mike

Michael Breslin
Kilpatrick Townsend & Stockton LLP
Suite 2800 | 1100 Peachtree Street NE | Atlanta, GA 30309-4528
office 404 685 6752 | fax 404 541 4749
mbreslin@kilpatricktownsend.com | My Profile | VCard

Comments to Plaintiff's proposed ESI search terms

Tranche 1

SIM
Subscriber identity module
Subscriber identification module
Hack!
Swap!
Intercept!
Compromise!
Scam!
Verif!
Impersonat!
Imposter
Pretend!
Fake!
Faking
Pose!
Posing
Breach!
Defraud!
Authoriz!
Unauthoriz!

Commented [BM1]: These terms are very generic and, if each is searched in isolation as you've proposed, will produce voluminous and almost exclusively irrelevant materials. The case involves unauthorized SIM changes and the search terms used should be designed to reflect that, like the terms we've proposed.

While we could see the reasonableness of certain of these terms if they were searched in connection with other terms that would make it likely they appear in a document concerning unauthorized SIM changes (for example "imposter" w/10 "SIM"), such documents should already be retrieved by the broad search we've proposed for all references to unauthorized SIM changes: ("SIM SWAP!" or "SIM HIJACK!" or ("SIM CHANGE!" w/2 (UNAUTHORIZ! or FRAUD!))).

We are happy to discuss these further. Also, if there are relevant documents that you hope to retrieve through these terms and that would not be captured by the terms we've proposed, please let us know what those are and we can discuss those as well.

Tranche 2

Customer w/10 secur!
Customer w/10 fraud!
Customer w/10 access!
Customer w/10 id
Customer w/10 ident!
Customer w/10 priv!
Account w/10 secur!
Account w/10 fraud!
Account w/10 access!
Account w/10 id
Account w/10 ident!
Account w/10 priv!
Data w/10 secur!
Data w/10 fraud!
Data w/10 access!
Data w/10 id
Data w/10 ident!
Data w/10 priv!
Information w/10 secur!
Information w/10 fraud!
Information w/10 access!
Information w/10 id
Information w/10 ident!
Information w/10 priv!
Information w/10 personal

Commented [BM2]: These terms appear designed to capture any document referencing account or data security, without regard to the context or any connection to SIM swapping or the issues in this case. AT&T has already produced its confidential account security, fraud prevention, and customer authentication procedures and training materials, which would cover all relevant information relating to the policies, procedures, and training applicable to the security of plaintiff's account and private information at the time of the incidents in this case. We don't see how these terms are reasonably tailored to capture additional documents relevant to the issues in the case.

If there are relevant documents that you hope to retrieve through these terms and that would not be captured by the terms we've proposed, or have not already been produced, please let us know what those are and we can discuss them.

Tranche 3

Prime
Alorica
TPUSA
Teleperformance
Concentrix
Convergys

Tranche 4

CPNI
Customer Proprietary Network Information

Tranche 5

Consent w/10 decree
Consent w/10 order
Comply w/10 decree
Comply w/10 order
Compliance w/10 decree
Compliance w/10 order
Compliance w/10 report
Compliance w/10 office!
Compliance w/10 plan!
FCC
Federal Communications Commission
Information Security Program
Risk Assessment

Commented [BM3]: Searching for any document containing only the name of any of these entities would return voluminous and almost exclusively irrelevant documents. We can see potential relevance in documents referencing these entities in connection with a discussion of the plaintiff or the SIM swaps in this case, but note that the search terms we've proposed would already capture all such documents, as they are designed to return any document referencing an unauthorized SIM change or Mr. Williams, or his account number or telephone number. Also, AT&T has already produced its master agreements with these entities and its policies and training materials applicable to these entities with respect to Plaintiff's account security and privacy.

If there are additional relevant materials you want to obtain regarding these entities, please specify what they are and we will be happy to discuss.

Commented [BM4]: Similar to the above, searching for all references to the term "CPNI" within a telecommunications company will return enormous amounts of irrelevant materials. While we could see the reasonableness of searching for documents referencing CPNI in connection with Mr. Williams or any activity on his AT&T account, the terms we've proposed are already broad enough to capture any such documents.

A more fundamental issue with these terms is there is still no evidence that any of Mr. Williams' CPNI was disclosed to any third party, let alone used in connection with any of the hacking incidents he alleges. Interrogatory No. 8 asked Mr. Williams to identify any of his CPNI that was disclosed, and his response only states that he believes "AT&T improperly provided third-party hackers with [his] SIM Card" and any CPNI that it may have contained. The account notes AT&T has produced demonstrate that is not what happened, and that Mr. Williams' SIM card was never removed (at least not be AT&T) from his phone. It was only Mr. Williams' service connection to the AT&T network that was transferred to a different phone/SIM card. Mr. Williams also has not produced any documents responsive to RFP No. 20, which requested materials indicating hackers used his CPNI to access any of his accounts.

If you have any evidence that Mr. Williams' CPNI was disclosed by AT&T to the hackers, please provide that to us. We are happy to discuss this issue further.

Commented [BM5]: The same problem exists for these terms, which appear designed to capture any document referencing the FCC or the 2015 Consent Decree (although, as worded, these terms as a whole will capture voluminous materials related to neither).

As we've indicated previously, we do not see any relevance in this case to the Consent Decree, which addressed two instances of vendor employees stealing SSNs to obtain phone unlock codes. And although the consent decree placed obligations on AT&T regarding protection of customer data, there is no evidence in this case that AT&T provided Mr. Williams' information to anyone, or that any information in AT&T's possession was used by the hackers to carry out their attacks on Mr. Williams.

Notwithstanding, AT&T has already produced its policies, procedures, and training materials related to account security and protection of customer information, from which Mr. Williams can assess AT&T's compliance with Section 222 or the applicable FCC Regulations.